19. The method of claim 1 wherein said transmitting said second digital data is performed via a wireless RF communication port associated with said portable electronic authorization device.

20. The method of claim 1 wherein said transmitting said second digital data is performed via a contact-type parallel communication port associated with said portable electronic authorization device.

21. A portable electronic authorization device for approving a transaction request originated from an electronic transaction system, comprising:

means for receiving at said portable electronic authorization device first digital data, said first digital data representing said transaction request;

means within said portable electronic authorization device for forming second digital data responsive to a receipt of said transaction request if a user of said portable electronic authorization device approves said transaction request, said second digital data representing encrypted data signifying said user's approval of said transaction request; and

means, coupled to said forming means, for transmitting said second digital data to said electronic transaction system.

22. The portable electronic authorization device of claim 21 wherein said second digital data includes at least a portion of said transaetion request.

23. The portable electronic authorization device of claim 21 further including first memory means eoupled to said forming means for storing a user's private key for use in forming said second digital data in accordance with a public key cryptography technique, wherein said forming means includes encrypting means coupled to said first memory means for creating said encrypted data with said user's private key using said public key cryptography technique, whereby said presence of said user's private key in said first memory means eliminates a need to exchange said user's private key between said portable electronic authorization devicc and said electronic transaction system for approving said transaction request.

24. The portable electronic authorization device of claim 23 further comprising key generation logic coupled to said first memory means for generating said user's private key within said portable electronic authorization device.

25. The portable electronic authorization device of claim 23 further comprising means, coupled to said first memory means, for configuring said portable electronic authorization device for said user, said configuring means receives configuration data from an issuer of an account capable of transaction via said portable electronic authorization device, said configuration data includes at least one of identification data pertaining said user and said private key; and

means for writing said configuration data to memory of said portable electronic authorization device.

26. The portable electronic authorization device of claim 21 further comprising:

means coupled to said forming means for authenticating said user prior to permitting said user to approve said transaction request using said portable electronic authorization device, said authenticating means requires one of a password, a finger print, and a voiee print.

27. The portable electronic authorization device of claim 21 wherein said means for transmitting said second digital data includes means for communicating with said electronic transaction system using infrared signals.

28. The portable electronie authorization device of claim 21 wherein said means for transmitting said second digital data includes means for communicating with said elcctronic transaction system using wireless RF signals.

29. The portable electronic authorization device of claim 21 wherein said means for transmitting said second digital data includes a contact-type serial port for communicating with said electronic transaction system.

30. The portable electronic authorization device of claim 21 wherein said means for transmitting said second digital data includes a contact-type parallel port for communicating with said electronic transaction system.

31. The portable eleetronic authorization device of claim 21 further comprising means, coupled to said receiving means, for displaying said transaction request for viewing by said user.

32. The portable electronic authorization device of claim 21 further comprising means, coupled to said forming means, for said user to indicate that said transaction request is approved, said means for said user to indicate that said transaction request is approved causes said second digital data to be transmitted from said portable elcctronic authorization device to said electronic transaction system.

33. The portable electronic authorization device of claim C10 wherein said means for said user to indicate that said transaction request is approved represents a switch configured for activation by said user.

34. The portable electronic authorization device of claim 21 wherein said first digital data represents an encrypted version of said transaction request, said first digital data being encrypted using public key cryptography with a private key associated with a transaction partner, wherein said means for receiving further comprising means for decrypting said first digital data using a public key associated with said transaction partner.

35. The portable electronic authorization device of claim 21 further comprising tamper-proof enclosure means for enclosing said receiving means, said forming means, and said transmitting means therein, said tamper-proof enclosure means being configured to prevent said user's private key from being extracted from said portable electronic authorization device if said tamper-proof enclosure means has been tampered with.

36. Thc portable electronic authorization dcvice of claim 21 wherein said means for receiving, means for forming, and means for transmitting are implemented on a single chip.

37. The portable electronic authorization device of claim 21 wherein said means for transmitting said second digital data includes a first PC card communication port associated with said portable electronic authorization device.

38. The portable electronic authorization device of claim 37 wherein said transaction request represents a transaction request for a transaction conducted via a computer network, said electronie transaction system includes a computer coupled to said computer network, said portable electronic authorization device being configured for plugging into a sccond PC card communication port of said computer to facilitate receiving said first digital data.

39. The portable electronic authorization device of claim 21 further including a power source for providing power to said forming means.

40. The portable electronic authorization device of claim 21 wherein said second digital data comprises at least a portion of said transaction request, said second digital data further eomprising identification data pertaining said user and a time stamp.

41. The portable electronic authorization device of claim 21 wherein said transaction request represents a request for authenticating an electronic file, said second digital data includes an electronic signature for authenticating said electronic file.

42. A portable electronic authorization device for approving a transaction request originated from an electronic transaction system, comprising:

first logic circuit configured to receive first digital data representative of said transaction request;

second logic circuit configured to form second digital data responsive to said transaction request received by said first logic circuit if said transaction request is approved by a user of said portable electronic transaction device, said second digital data representing encrypted data signifying an approval by said user of said transaction request; and

transmission circuitry coupled to said second logic circuit, said transmission eircuitry being configured to transmit said second digital data from said portable electronic authorization apparatus to said electronic transaction system if said user approves said transaction request.

43. The portable electronic authorization device of claim 42 wherein said second digital data includes at least a portion of said transaction request.

44. The portable electronic authorization device of claim 42 wherein said first digital data represents an encrypted version of said transaction request, said first digital data being enerypted using public key cryptography with a private key associated with a transaction partner, wherein said first logic circuit comprises decrypting circuitry configured to decrypt said first digital data using a public key associated with said transaction partner.

45. Thc portable electronic authorization device of claim 44 further including first memory circuit coupled to said decrypting circuitry, said first memory circuit being configured for storing a user's private key for use in forming said second digital data in accordance with a public key cryptography technique, wherein said seeond logic cireuit includes encrypting logic coupled to said first memory circuit for creating said encrypted data with said user's private key using said public key cryptography technique, whereby said presence of said user's private key in said first memory circuit eliminates a need to exchange said user's private kcy between said portable electronic authorization device and said electronic transaction system for approving said transaction rcquest.

46 The portable electronic authorization device of claim 45 further comprising key generation logic coupled to said first memory means for generating said user's private key within said portable electronic authorization device.

47 The portable electronic authorization device of claim 46 wherein said first logic circuit comprises receiving circuit coupled to said decrypting logic, said receiving circuit being configured to receive said first digital data from said electronic transaction system prior to passing said first digital data to said decrypting logic for decryption, said receiving circuit being decoupled from said first memory circuit, wherein said user's private key stored in said first memory circuit is inaccessible directly by said receiving logic, thereby preventing said user's private key from being accessed from externally without traversing said decrypting logic.

48 The portable electronic authorization device of claim 47 wherein said transmission circuitry is decoupled from said first memory circuit, wherein said user's private key stored in said first memory circuit is inaccessible directly by said transmission circuit, thereby preventing said user's private key from being accessed from externally without traversing one of said decrypting logic and said encrypting logic.

49. The portable electronic authorization device of claim 42 further comprising:

user authentication meehanism coupled to said second logic circuit, said user authentication mechanism being configured to authenticate said user prior to permitting said user to approve said transaction request using said portable electronic authorization device, said authentication mechanism requires one of a password, a finger print, and a voice print.

50. The portable electronic authorization device of claim 42 wherein said transmission circuitry includes circuitry configured for communicating with said electronic transaction system using infrared signals.

51. The portable eleetronic authorization device of elaim 42 wherein said transmission circuitry includes circuitry configured for communicating with said electronic transaction system using wireless RF signals.

52. The portable electronic authorization device of claim 42 wherein said transmission circuitry includes a contact-type serial port for communicating with said electronic transaction system.

53. Thc portable eleetronic authorization device of claim 42 wherein said transmission circuitry includes a contact-type parallel port for communicating with said electronic transaction system.

54. The portable electronic authorization device of claim 42 further comprising a display coupled to said first logic circuit, said display being configured to display said transaction request for viewing by said user.

55. The portable electronic authorization device of claim 42 further comprising a switch eoupled to said second logic cireuit, said switch permitting said user to indicate through activating said switch that said transaction request is approved by said user.

56. The portable electronic authorization device of claim 42 further comprising tamper-proof enclosure for enclosing said first logic circuit, said second logic circuit, and said transmission circuitry therein, said tamper-proof enclosure being configured to prevent said user's private key from being extracted from said portable electronic authorization device if said tamper-proof enclosure has been tampered with.

57. The portable electronic authorization device of claim 42 wherein said first logic circuit, said second logic circuit, and said transmission circuitry are implemented on a single chip.

58. The portable electronic authorization device of claim 42 wherein said transmission circuitry includes a PC card communication port associated with said portable electronic authorization device.

59. The portable electronic authorization device of claim 58 wherein said transaction request represents a transaction request for a transaction conducted via a computer network, said electronic transaction system includes a computer coupled to said computer network, said

portable electronic authorization device being configured for plugging into a PC card slot of said computer to facilitate receiving said first digital data.

60. The portable electronic authorization device of claim 42 further including a power source to facilitate portability.

61. The portable electronic authorization device of claim 42 wherein said second digital data comprises at least a portion of said transaction request, said second digital data further comprising identification data pertaining said user and a time stamp.

62. The portable electronic authorization device of claim 42 wherein said transaction request represents a request for authenticating an electronic file, said second digital data includes an electronic signature for authenticating said electronic file.

63. In a portable electronic authorization device, a method for approving a transaction request originated from an electronic transaction system, comprising:

receiving at said portable electronic authorization device first digital data, said first digital data representing said transaction request;

if said transaction request is approved by a user of said portable electronic authorization device, generating second digital data, said second digital data representing transaction approval data signifying said user's approval of said transaction request;

encrypting within said portable electronic authorization device said second digital data, thereby creating third digital data representing an encrypted version of said second digital data; and

transmitting said third digital data from said portable electronic authorization device to said electronic transaction system, thereby permitting said electronic transaction system to ascertain whether said transaction request is approved by said user.

64. The method of claim 63 wherein said encrypting is performed using a public key cryptography technique, said portable electronic authorization device containing a user's private

key for encrypting said second digital data to form said third digital data, thereby eliminating a need to transmit said user's private key from said portable electronic authorization device to said electronic transaction system, said third digital data being configured for being decrypted at said electronic transaction system using a user's public key.

65 The method of claim 64 wherein said user's private key is generated by a key generation logic within said portable electronic authorization deviee.

66. The method of claim 63 further comprising:

authenticating said user prior to permitting said user to approve said transaction request using said portable electronic authorization device, said authenticating requires one of a password, a finger print, a voice print at a user authentication mechanism associated with said portable electronic authorization device.

67. The method of claim 63 wherein said user's private key is generated using a key generation logic within said portable eleetronic authorization device, thereby eliminating a need to transmit said user's private key from said electronic transaction system to said portable electronic authorization device.

68. The method of claim 63 wherein said transmitting said third digital data is performed via an infrared communication port associated with said portable electronic authorization device.

69. The method of claim 63 wherein said transmitting said third digital data is performed via a wireless RF communication port associated with said portable electronic authorization device.

70. The method of claim 63 wherein said transmitting said third digital data is performed via a contact-type parallel eommunication port associated with said portable electronic authorization device.

71. The method of claim 63 wherein said transmitting said third digital data is performed via a contact-type serial communication port associated with said portable electronic authorization device.

72. The method of elaim 63 further comprising displaying said transaction request for viewing by said user on a display screen associated with said portable electronic authorization device.

73. The method of claim 63 further comprising activating an approval switch associated with said portable electronic authorization device if said transaction request is approved by said user.

74. The method of claim 63 wherein said first digital data represents an encrypted version of said transaction request encrypted using public key cryptography, wherein said receiving further comprising decrypting, using decryption logic associated with said portable eleetronic authorization device, said first digital data using a transaction partner's public key .

75. The method of claim 63 wherein said portable electronic authorization device is enclosed in a tamper-proof enclosure, said tamper-proof enclosure being configured to prevent said user's private key from being extracted from said portable electronic authorization device if said tamper-proof enclosure has been tampered with.

76. The method of claim 63 wherein said portable electronic authorization device is implemented on a single chip.

77. The method of claim 63 wherein said transmitting said third digital data is performed via a PC card communication port associated with said portable electronic authorization device.

78. The method of claim 77 wherein said transaction request represents a transaction request for a transaction conducted via a computer network, said electronic transaction system includes a computer coupled to said computer network, said portable electronic authorization device configured for plugging into a PC eard slot of said computer to facilitate said receiving said first digital data.

79. The method of claim 63 wherein said portable electronic authorization device is configured for portability and includes a power source.

80. The method of claim 63 wherein said transaction approval data comprises at least a portion of said transaction rcquest, said transaction approval data further comprising identification data pertaining said user and a time stamp.

81. The method of claim 63 further eomprising configuring said portable electronic authorization device for said user by receiving configuration data from an issucr of an account capable of transaction via said portable electronic authorization device, said configuration data includes at least one of identification data pertaining said user and said private key.

82. The method of claim 63 wherein said transaction request represents a request for authenticating an electronic file, said transaction approval data includes an electronic signature attached to said electronic file.

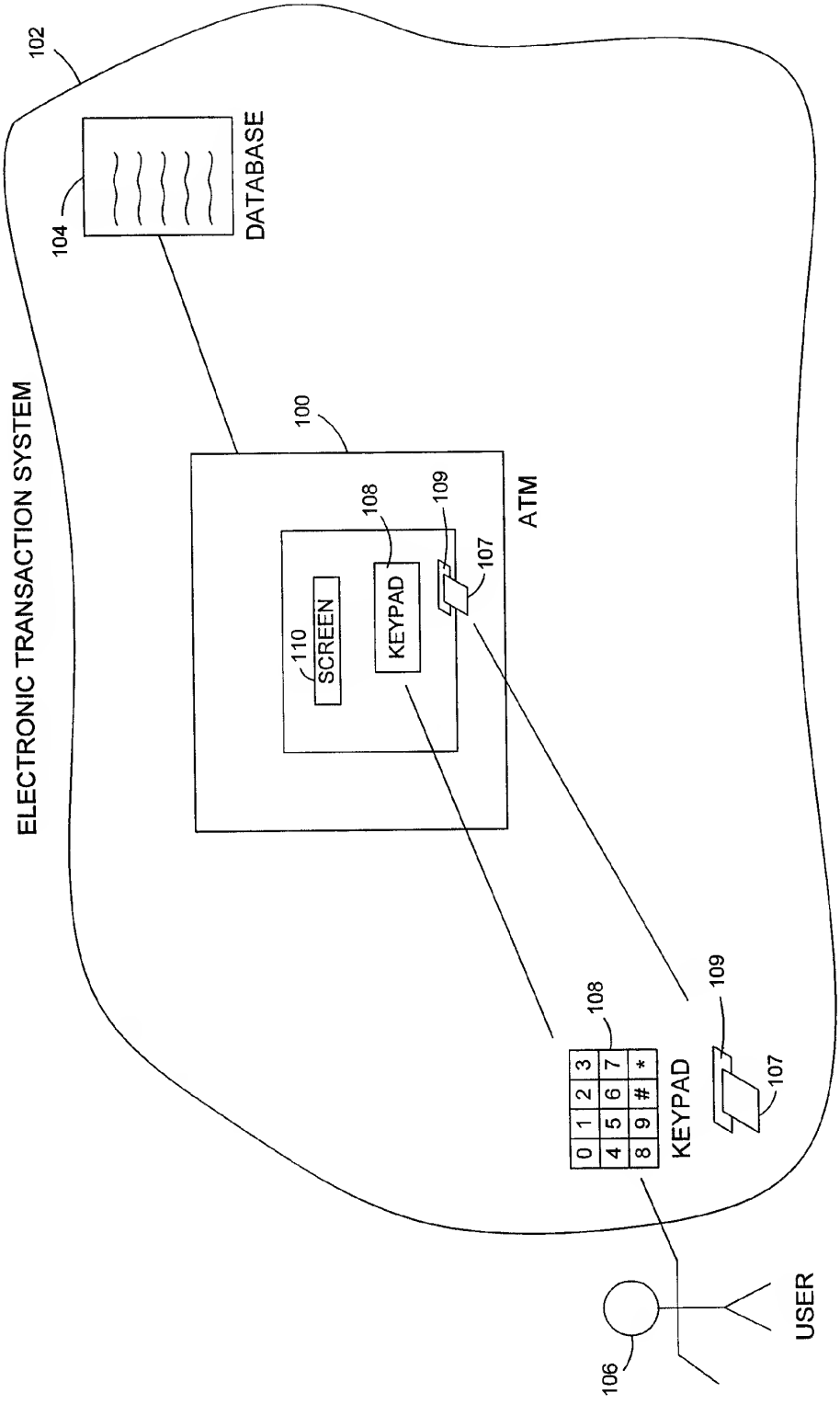


FIG. 1 (PRIOR ART)

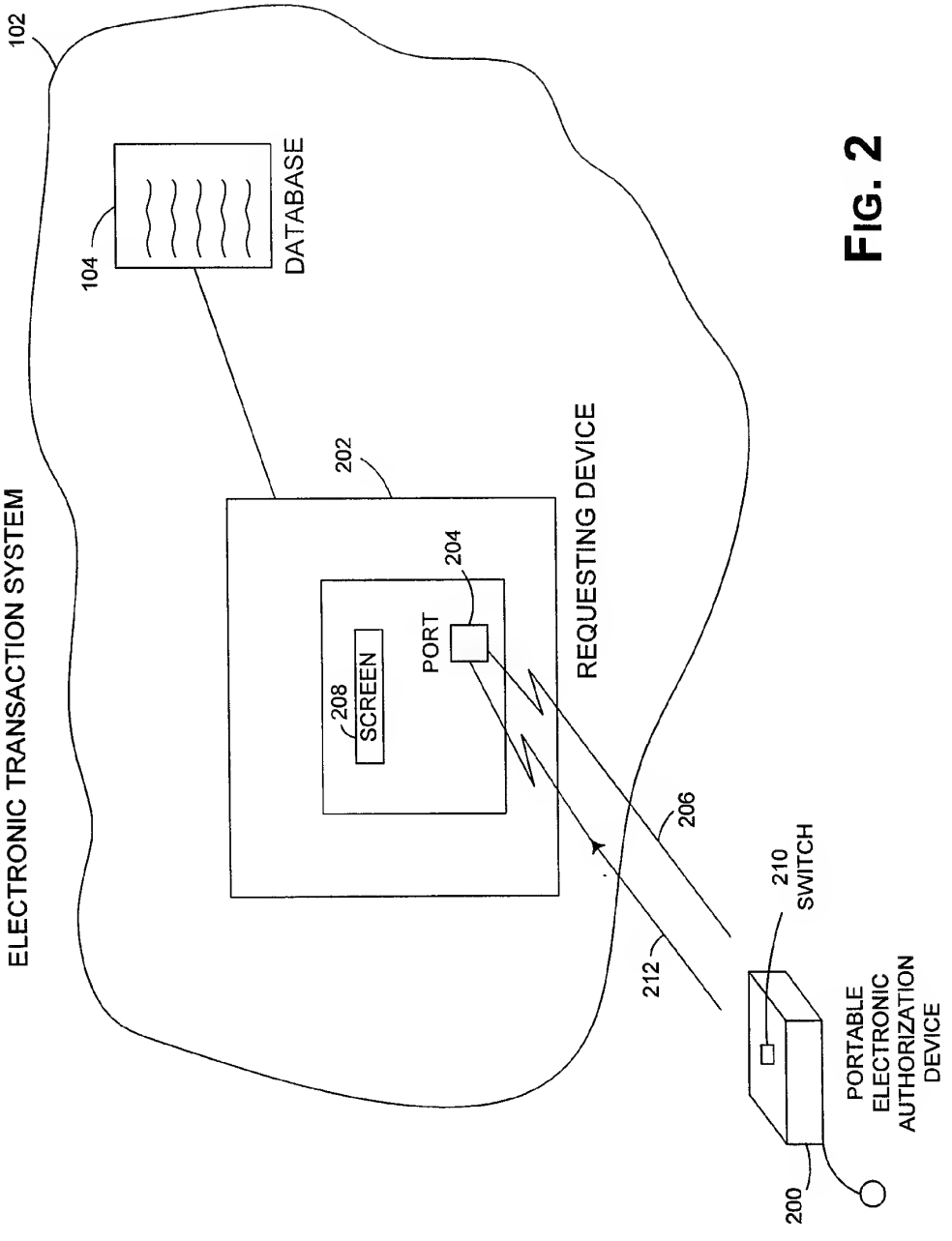

ELECTRONIC TRANSACTION SYSTEM
102
DATABASE
104
REQUESTING DEVICE
202
204
PORT
208
SCREEN
206
212
210
SWITCH
PORTABLE ELECTRONIC AUTHORIZATION DEVICE
200

FIG. 2

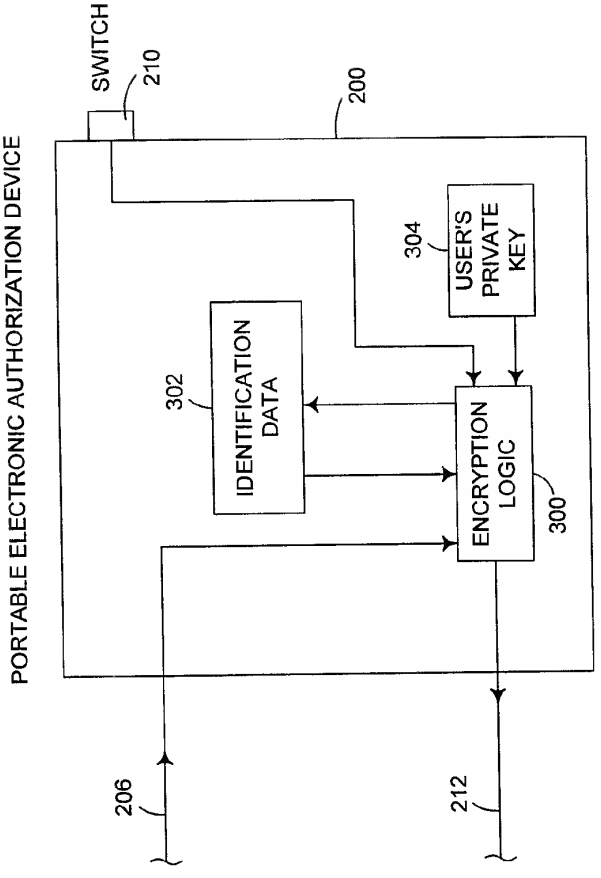

PORTABLE ELECTRONIC AUTHORIZATION DEVICE
SWITCH
210
200
304
USER'S PRIVATE KEY
302
IDENTIFICATION DATA
ENCRYPTION LOGIC
300
206
212

FIG. 3A

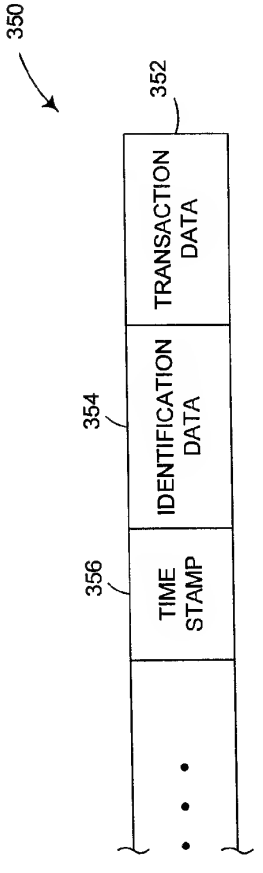

350
352
TRANSACTION DATA
354
IDENTIFICATION DATA
356
TIME STAMP

FIG. 3B

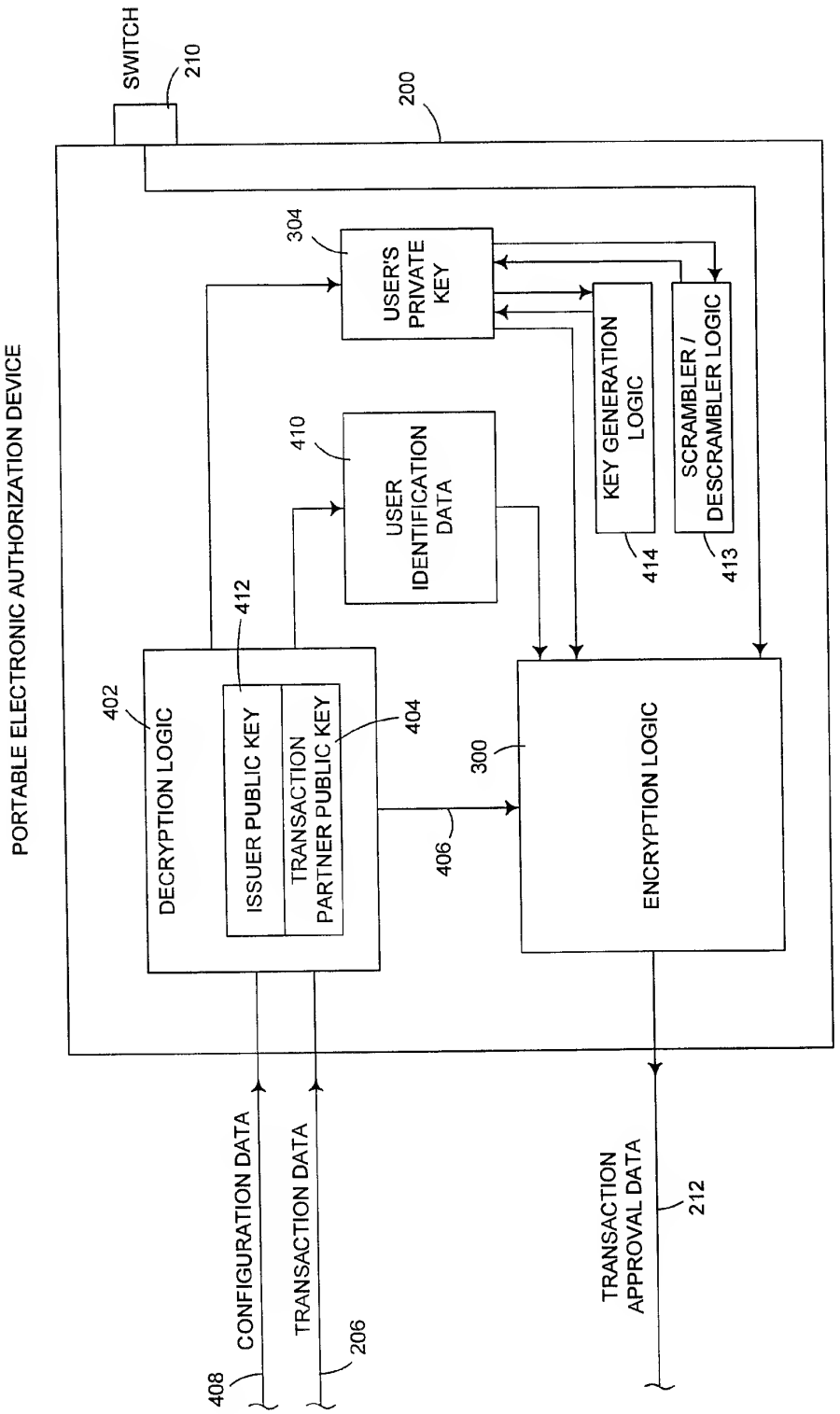

PORTABLE ELECTRONIC AUTHORIZATION DEVICE
SWITCH
210
200
304
USER'S PRIVATE KEY
410
USER IDENTIFICATION DATA
KEY GENERATION LOGIC
414
SCRAMBLER / DESCRAMBLER LOGIC
413
412
402
DECRYPTION LOGIC
ISSUER PUBLIC KEY
TRANSACTION PARTNER PUBLIC KEY
404
406
300
ENCRYPTION LOGIC
CONFIGURATION DATA
408
TRANSACTION DATA
206
TRANSACTION APPROVAL DATA
212

FIG. 4

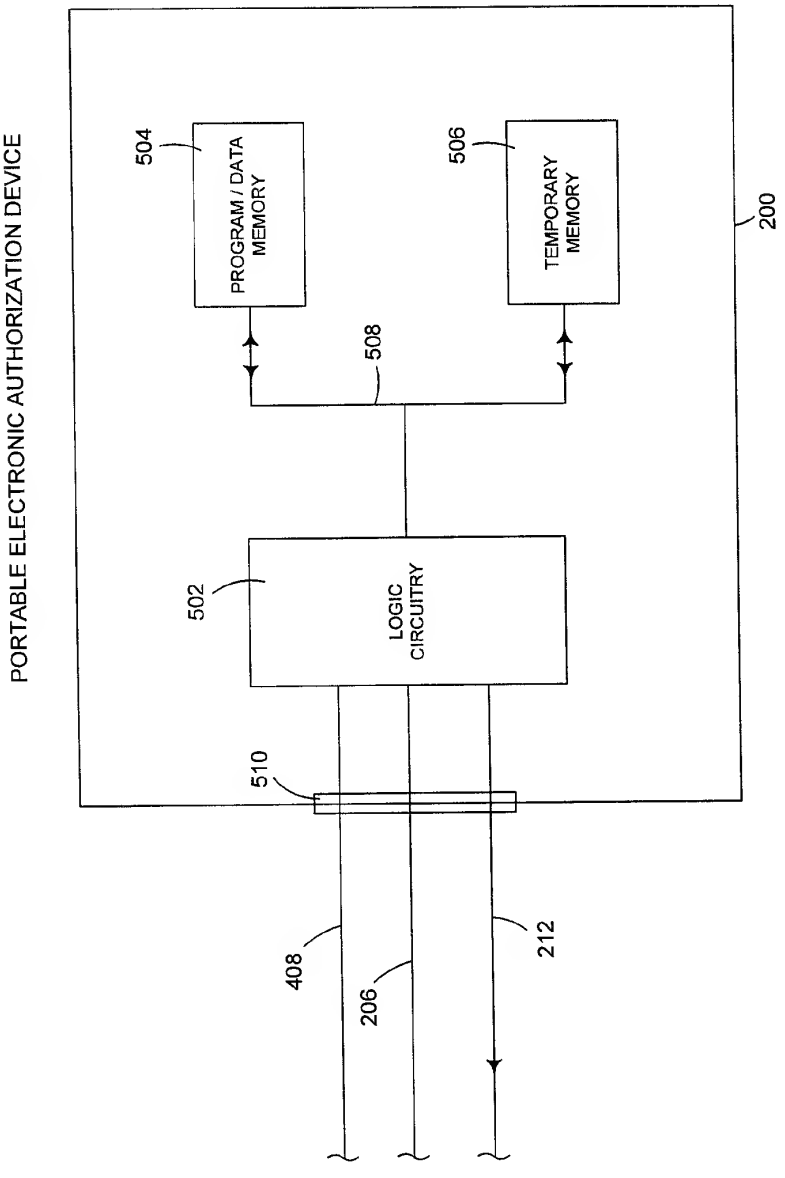

PORTABLE ELECTRONIC AUTHORIZATION DEVICE
504
PROGRAM / DATA MEMORY
506
TEMPORARY MEMORY
200
508
502
LOGIC CIRCUITRY
510
408
206
212

FIG. 5A

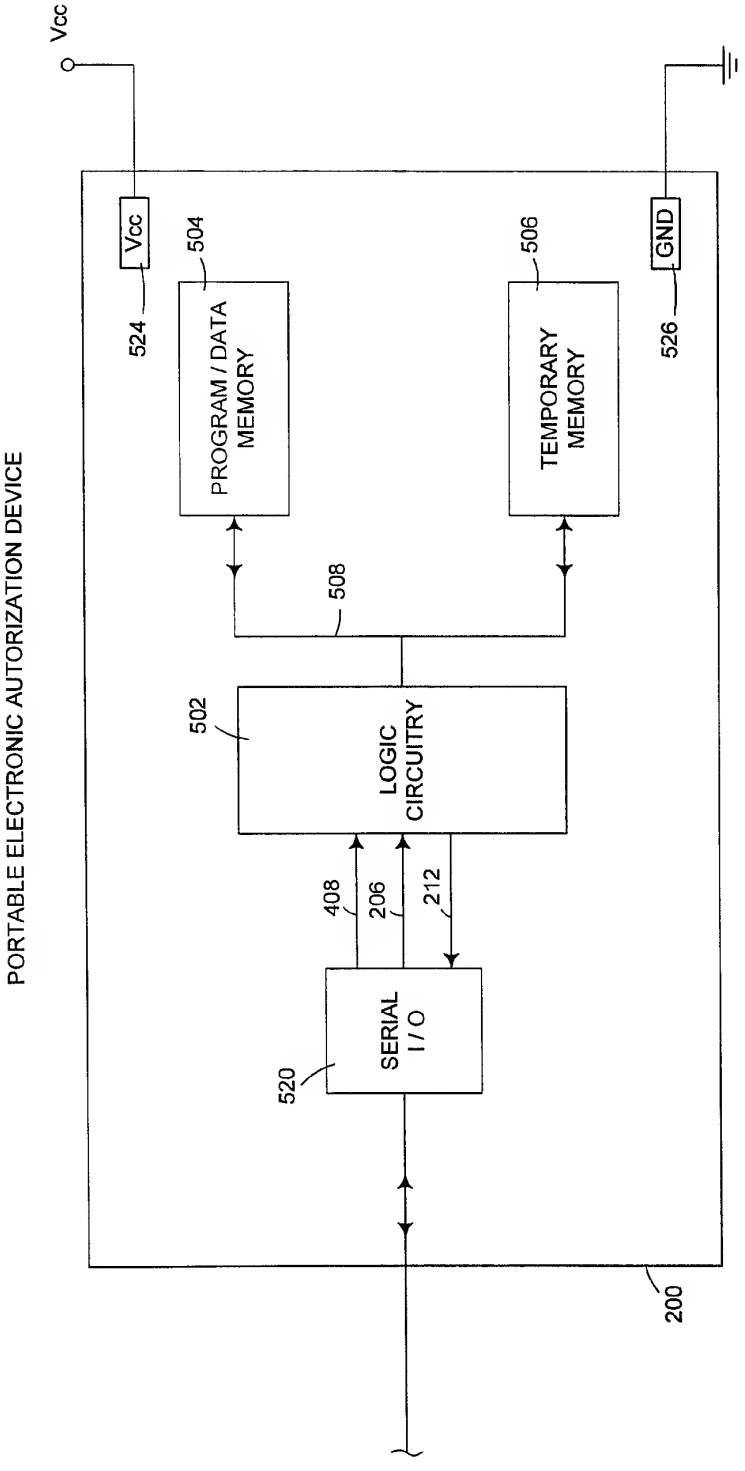
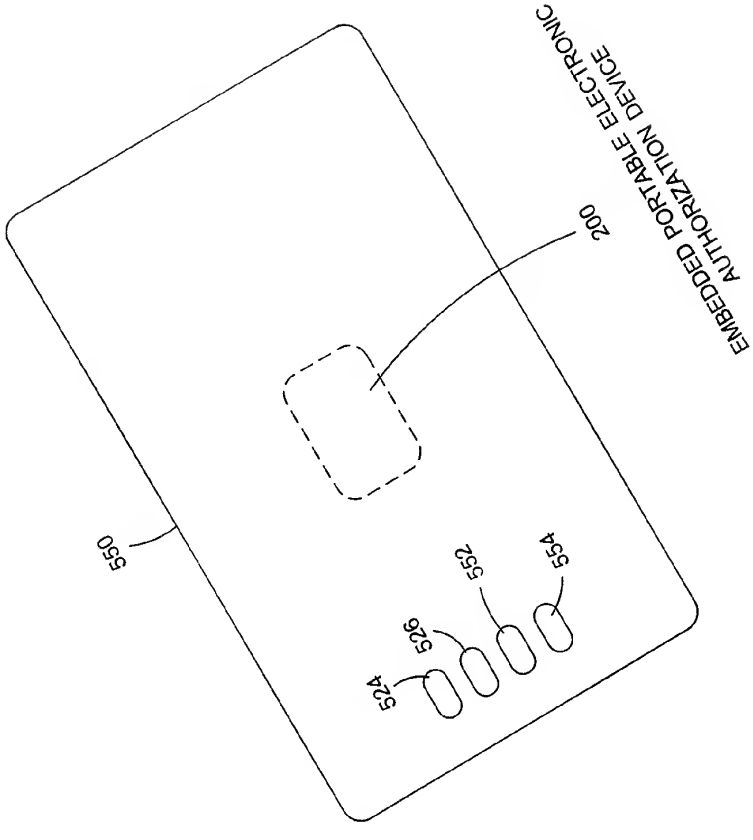

PORTABLE ELECTRONIC AUTORIZATION DEVICE
Vcc
Vcc
524
504
PROGRAM / DATA MEMORY
506
TEMPORARY MEMORY
GND
526
508
502
LOGIC CIRCUITRY
408
206
212
520
SERIAL I / O
200

FIG. 5B

FIG. 5C


EMBEDDED PORTABLE ELECTRONIC AUTHORIZATION DEVICE
200
550
554
552
526
524

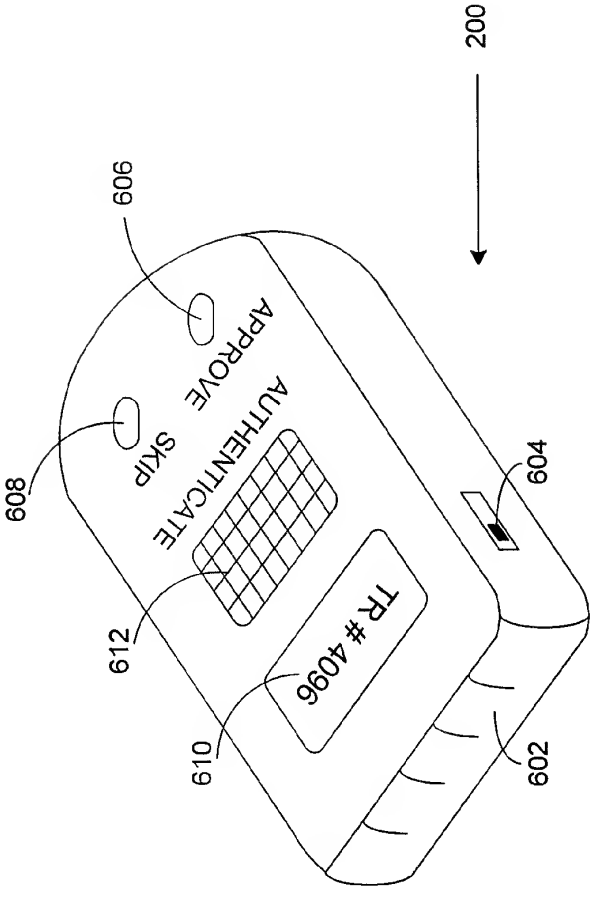

200
606
APPROVE
SKIP
AUTHENTICATE
608
604
612
TR # 4096
610
602

FIG. 6A

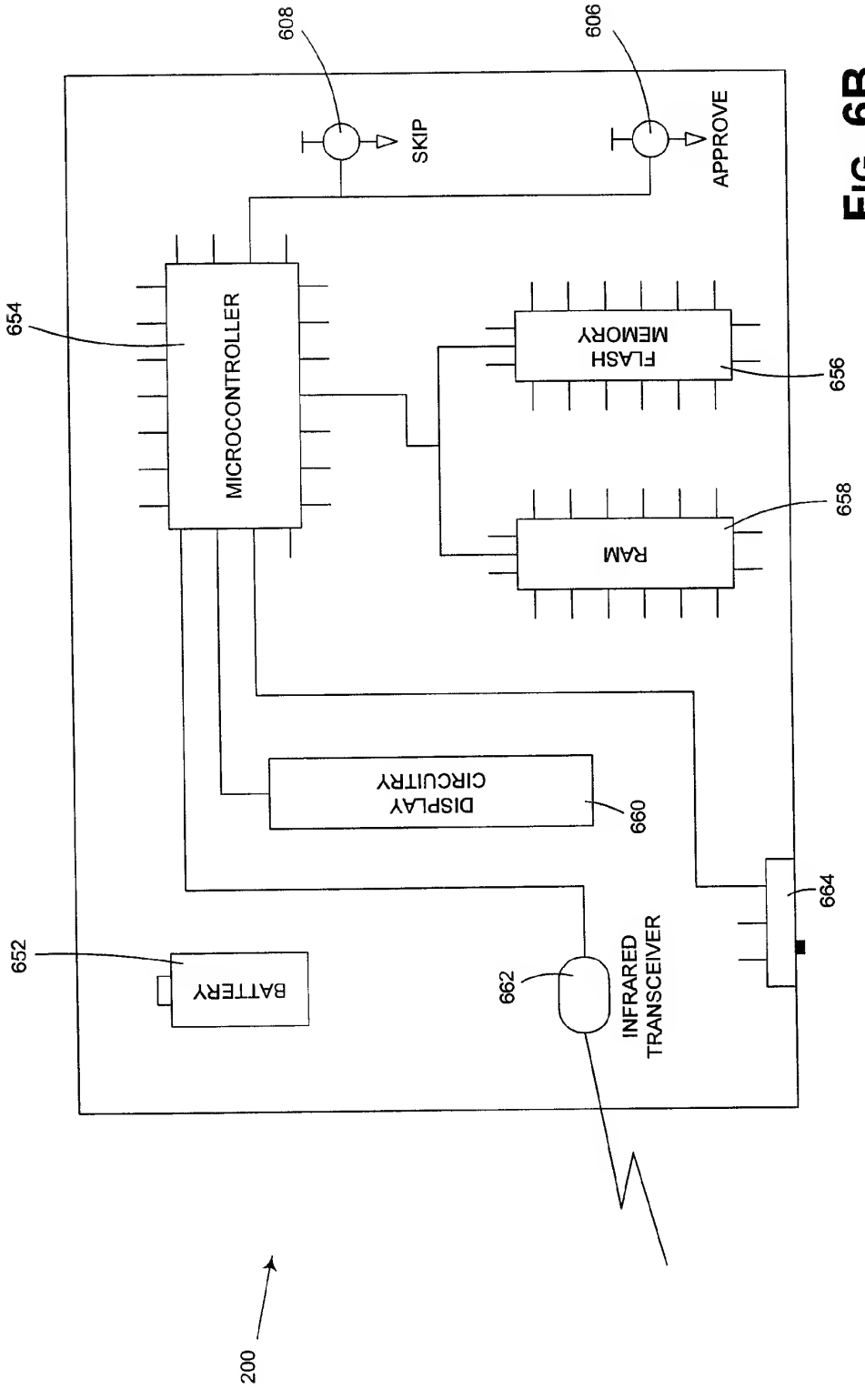

608
606
SKIP
APPROVE
654
MICROCONTROLLER
FLASH MEMORY
656
658
RAM
DISPLAY CIRCUITRY
660
664
652
BATTERY
662
INFRARED TRANSCEIVER
200

FIG. 6B

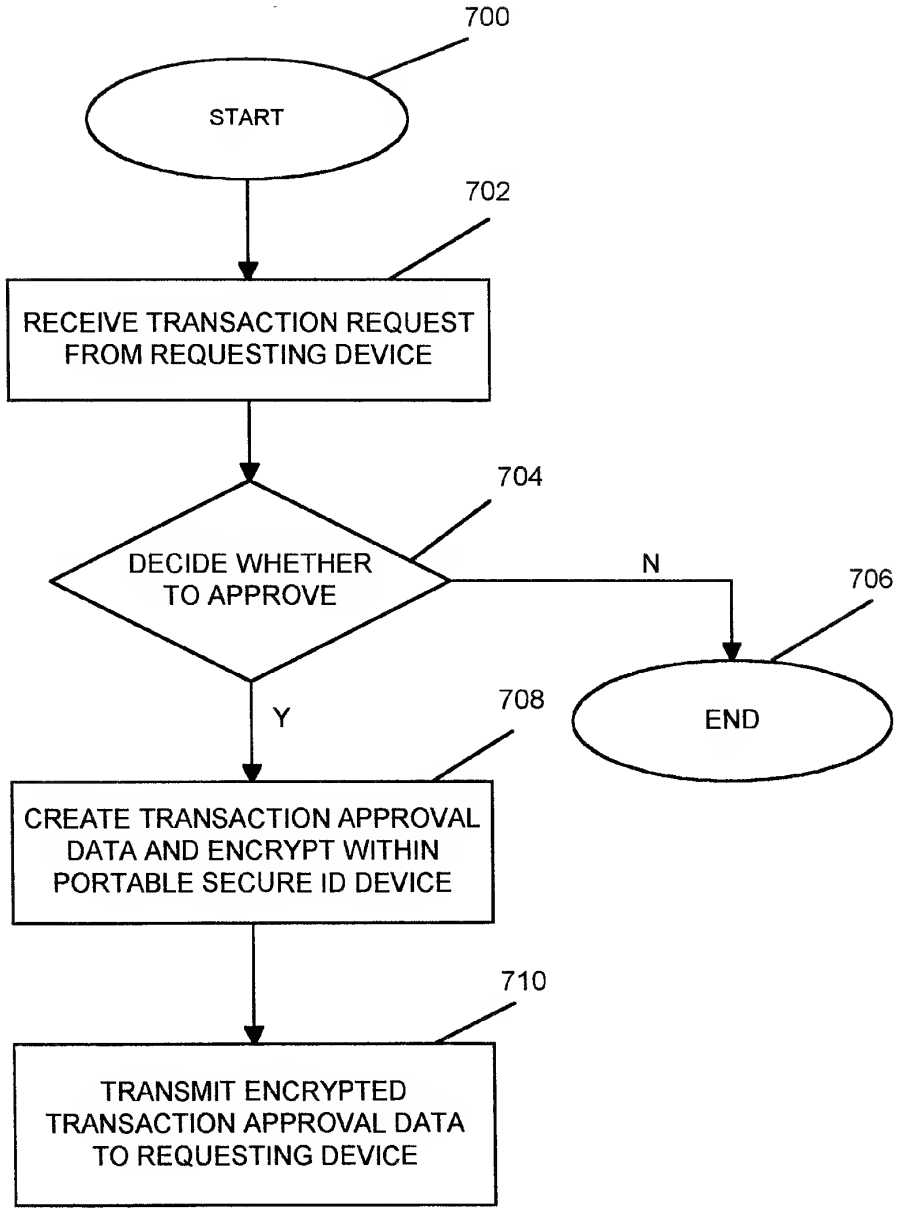

700
START
702
RECEIVE TRANSACTION REQUEST FROM REQUESTING DEVICE
704
DECIDE WHETHER TO APPROVE
N
706
END
Y
708
CREATE TRANSACTION APPROVAL DATA AND ENCRYPT WITHIN PORTABLE SECURE ID DEVICE
710
TRANSMIT ENCRYPTED TRANSACTION APPROVAL DATA TO REQUESTING DEVICE

FIG. 7

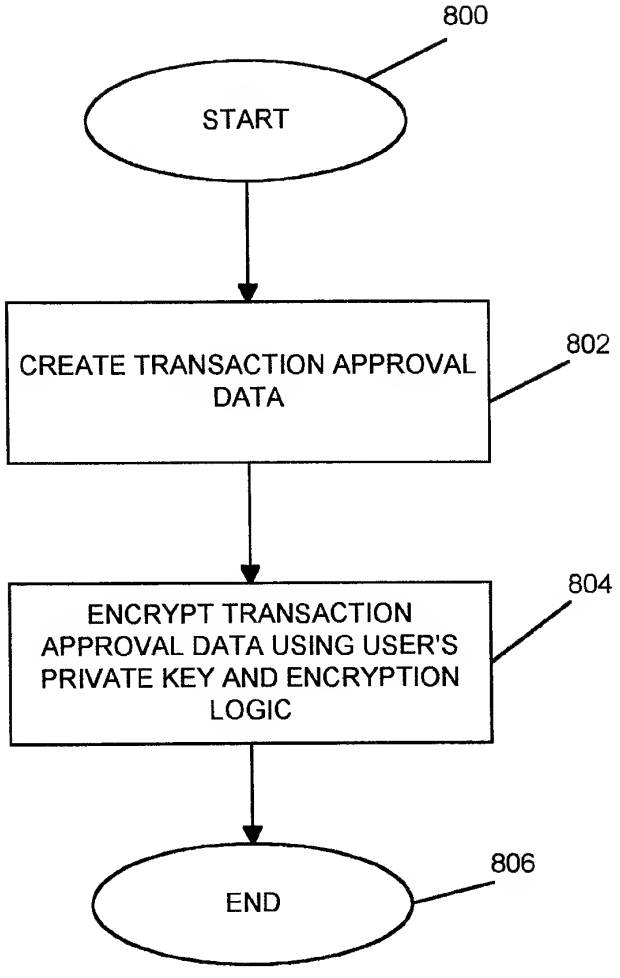

800
START
CREATE TRANSACTION APPROVAL DATA
802
ENCRYPT TRANSACTION APPROVAL DATA USING USER'S PRIVATE KEY AND ENCRYPTION LOGIC
804
END
806

FIG. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/23125

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04K 1/00, H04L 9/00

US CL :380/23, 25, 30; 235/382

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/23, 25, 30, 24, 4, 49, 28, 21; 235/382, 380

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,373,561 A (HABER et al.) 13 December 1994	1-82
A	US 5,548,106 A (LIANG et al.) 20 August 1996	1-82
A	US 5,524,052 A (AUGUSTINE et al.) 04 June 1996	1-82
A	US 5,455,863 A (BROWN et al.) 03 October 1995	1-82
A	US 5,440,633 A (AUGUSTINE et al.) 08 August 1995	1-82
A	US 5,416,842 A (AZIZ) 16 May 1995	1-82
A, P	Fancher, "In your Pocket Smartcards", IEEE Spectrum February 1997, pp 47-53	1-82

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 23 MARCH 1998	Date of mailing of the international search report 05 MAY 1998
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer DAVID CAIN Telephone No. (703) 305-1836

Form PCT/ISA/210 (second sheet)(July 1992)★

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/23125

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X, E	US 5,724,423 A (KHELLO) 03 March 1998, column 6, line 31 - column 16 line 61.	1-82
A, P	US 5,623,637 A (JONES, et al.) 22 April 1997	1-82